

# Lecture Outline

- Finish broader notions relating to authentication:
  - Multi-party identities (Ecommerce, web advertising)
  - Bot-or-Not (CAPTCHAs)
- Project status reports
- Botnets:
  - Basic structure
  - More sophisticated C&C
  - *Bulletproof hosting*
  - *Pay-per-Install* (PPI)

Multi-Party Identities, con't

# Better Fix for CAAS Attack #2

S→M: `place_order.html`  
*[M inserts ID and price into database]*

Principle: always sign  
all the information that  
went into a decision

M→S→C: `get_payment?`  
`SIGNM(ID=X, price=Y, merch=M, shop=S)`  
*[C verifies signature; records payment info, generates # T]*

C→S→M: `finish?`  
`SIGNC(ID=X, price=Y, merch=M, shop=S, PAID)`  
*[M verifies signature and PAID is indicated, etc.]*  
*[M retrieves orderID=X from database;*  
*if order status = PENDING → mark as PAID; ship X]*

# CAAS Attack #3 ?

...

$S \rightarrow M$ : checkout?ID= $X$ &price= $Y$

[ $M$  sets session\_status[ $S$ ]  $\leftarrow$   
confirm\_with\_C(shop= $S$ , ID= $X$ , price= $Y$ ) ]

$M \rightarrow S \rightarrow M$ : update\_status?SIGN <sub>$M$</sub> ( ID= $X$ )

[ $M$  validates signature;  
if session\_status[ $S$ ] = **CONFIRMED**  $\rightarrow$   
session\_status[ $S$ ] = **PAID**; ship  $X$ ]



# CAAS Attack #3 !

S→M: checkout?ID= $X_1$ &price= $Y_1$

[M sets session\_status[S] ←  
confirm\_with\_C(...,  $X_1$ ,  $Y_1$ ) ← **FAILED**]

M→S: update\_status?SIGN<sub>M</sub>(ID= $X_1$ )

S→M: checkout?ID= $X_2$ &price= $Y_2$   $Y_2 \ll Y_1$

[M sets session\_status[S] ←  
confirm\_with\_C(...,  $X_2$ ,  $Y_2$ ) ← **CONFIRMED**]

S→M: update\_status?SIGN<sub>M</sub>(ID= $X_1$ )

[M validates signature;  
if session\_status[S] = **CONFIRMED** →  
session\_status[S] = **PAID**; ship  $X_1$ ]

# Fix for CAAS Attack #3

S → M: checkout?ID= $X_1$ &price= $Y_1$   
[M sets session\_status[S,  $X_1$ ] ←  
confirm\_with\_C(...,  $X_1$ ,  $Y_1$ ) ← **FAILED**]

M → S: update\_status?SIGN<sub>M</sub>(ID= $X_1$ )

S → M: checkout?ID= $X_2$ &price= $Y_2$   $Y_2 \ll Y_1$   
[M sets session\_status[S,  $X_2$ ] ←  
confirm\_with\_C(...,  $X_2$ ,  $Y_2$ ) ← **CONFIRMED**]

S → M: update\_status?SIGN<sub>M</sub>(ID= $X_1$ )

[M validates signature;

~~if session\_status[S,  $X_1$ ] = **CONFIRMED** →  
session\_status[S] = **PAID**; ship  $X_1$ ]~~

# Better Fix for CAAS Attack #3

S→M: checkout?ID= $X_1$ &price= $Y_1$

[M sets session\_status[S,  $X_1$ ,  $Y_1$ ] ←  
confirm\_with\_C(...,  $X_1$ ,  $Y_1$ ) ← **FAILED**]

M→S: update\_status?SIGN<sub>M</sub>(ID= $X_1$ ,  $Y_1$ )

S→M: checkout?ID= $X_2$ &price= $Y_2$   $Y_2 \ll Y_1$

[M sets session\_status[S,  $X_2$ ,  $Y_2$ ] ←  
confirm\_with\_C(...,  $X_2$ ,  $Y_2$ ) ← **CONFIRMED**]

S→M: update\_status?SIGN<sub>M</sub>(ID= $X_1$ ,  $Y_1$ )

[M validates signature;

~~if session\_status[S,  $X_1$ ,  $Y_1$ ] = **CONFIRMED** ✗~~





~~session\_status[S] ← **PAID**; ship  $X_1$ ]~~

# Imposing Identity, Part 1

How web-based advertising is supposed to work:

1. You have a web site about say kittens
2. In it, you link to Amazon kitten products
3. *If* a user clicks on the link, it includes your **affiliate ID**
4. Amazon notes ID, reflects it in a cookie sent to user



	Amazon's Choice		
			
Upsky Cat Toy Roller Cat Toys 3 Level Towers Tracks Roller with Six Colorful Ball Interactive Kitten Fun Mental Physical...	Pet Mate 42036 Arm & Hammer Large Sifting Litter Pan	Rainbow Cat Charmer	Burt's Bees Tearless Kitten Shampoo with Buttermilk
★★★★☆ ~ 5,222	★★★★☆ ~ 4,071	★★★★☆ ~ 4,395	★★★★☆ ~ 356
\$6 <sup>99</sup>	\$15 <sup>49</sup> \$16.83	\$5 <sup>64</sup> \$6.49	\$5 <sup>93</sup>
FREE Delivery for Prime members	✓prime FREE Delivery Thu, Apr 2 More Buying Choices \$14.25 (6 used & new offers)	✓prime FREE Delivery Thu, Apr 2 Other fast & free options with Prime: Amazon Fresh	Save 5% more with Subscribe & Save ✓prime FREE Delivery Thu, Apr 2

# Imposing Identity, Part 1

How web-based advertising is supposed to work:

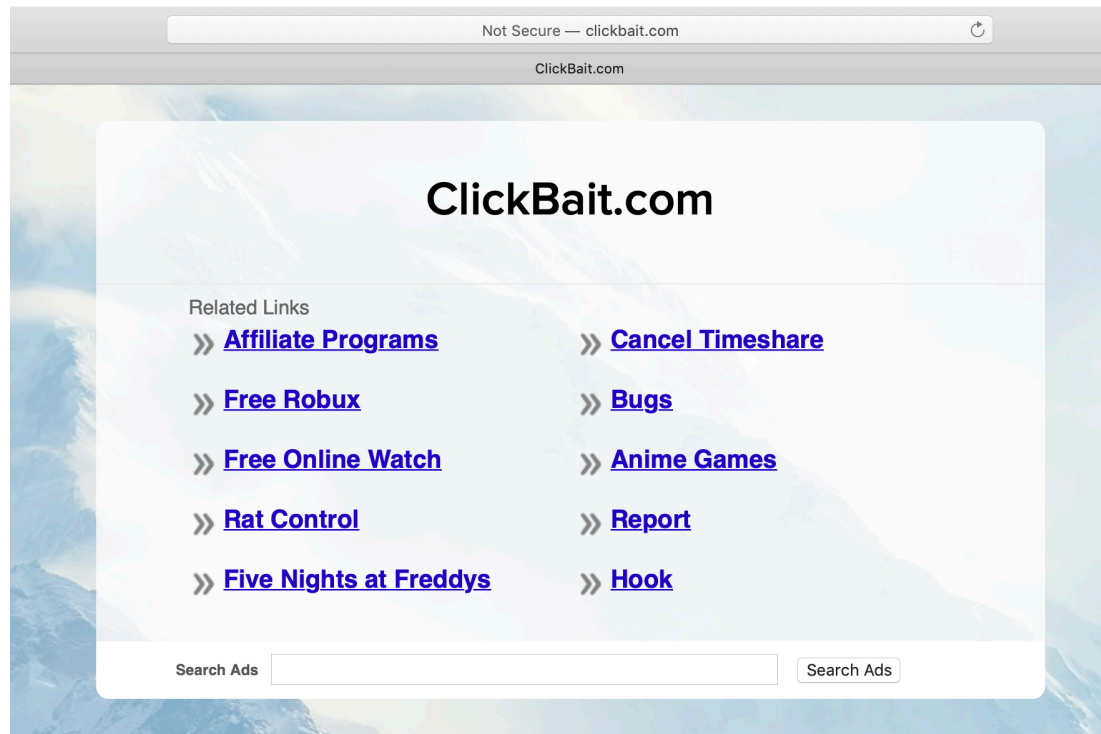
1. You have a web site about say kittens
2. In it, you link to Amazon kitten products
3. *If* a user clicks on the link, it includes your affiliate ID
4. Amazon notes ID, reflects it in a cookie sent to user
5. ... (user leaves your site, time passes) ...
6. *If* user subsequently buys (broadly interpreted),  
cookie gives you credit
7. Profit!



# Imposing Identity, Part 2

Suppose instead you have (a) no kitten web site and (b) no scruples:

1. But you have *some* sort of site that gets some traffic ...  
1'. ... or you say send spam to get users to execute your HTML





# Imposing Identity, Part 2

Suppose instead you have (a) no kitten web site and (b) no scruples:

1. But you have *some* sort of site that gets some traffic ...  
1'. ... or you say send spam to get users to execute your HTML
2. Your HTML causes the users browser to automatically visit Amazon w/ your **affiliate ID**
3. Amazon notes ID, reflects it in a cookie sent to user
4. ... (user leaves your site/junks your spam, time passes)...
5. *If* user happens to subsequently buy (broadly interpreted) for whatever reason, cookie **gives you credit**
6. **Profit!**

# Cookie Stuffing

BUSINESS  
INSIDER

eBay alleged that what Hogan did was to get the knock at his door by the FBI and that he had falsely credited him for sales he

Very hard to defend against 😞.  
Can't rely on Referer (HTTPS).  
No indication in HTTP GET of  
*organic vs. automation.*

seeding unknowing users with hundreds of thousands of bits of tracking code, or "cookies." If any of those people bought something on eBay, the code signaled to eBay that Hogan should get a cut of the sale — even though he had done nothing to promote eBay.

The sting also netted Brian Dunning, eBay's second biggest affiliate marketer. The company had paid Hogan and Dunning a combined \$35 million in commissions over the years, court papers say. Both men have since pleaded guilty to wire fraud.



# Bot-or-Not: CAPTCHAs

vatinkes πύργους



stop spam.  
read books.

### Verify Your Registration

- Enter the code shown:

[More info](#)

This helps prevent automated registrations.



Please enter the code you see below. [what's this?](#)



### Qualifying question

Just to prove you are a human, please answer the following math challenge.

Q: Calculate:

$$\frac{\partial}{\partial x} \left[ 4 \cdot \sin \left( 7 \cdot x - \frac{\pi}{2} \right) \right] \Big|_{x=0}$$

A:

mandatory

Note: If you do not know the answer to this question, reload the page and you'll get another question.



Figure 2: Difficult but correctly transcribed examples from the internal street numbers dataset.

Solveable by Google Street View in 2014



Figure 4: Examples of images from the hard CAPTCHA puzzles dataset.

Solveable by Google Street View in 2014

# Properties of Identities: Human or Bot?

- Issues with *CAPTCHAs*?
  - **Arms race**: getting harder & harder for humans to solve
  - **Accessibility**
  - Enabling **benign robots**
  - Core problem: ***outsourcing***



"crack captcha"  
.....

**crack captcha php**

Google Search

I'm Feeling Lucky

[Advanced Search](#)  
[Language Tools](#)

[Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2009 - [Privacy](#)



"crack captcha"

Search

[Advanced Search](#)

Web [+ Show options...](#)

Results 1 - 10 of about 17,700 for "[crack captcha](#)". (0.17 seconds)

[Captcha solving](#)

Sponsored Link

[www.decaptcher.com](http://www.decaptcher.com) Cheap captcha solving Cheap programs for advertisement

Using the advertisement in blogs, social networks, etc significantly increases the efficiency of the business. Many services use pictures called CAPTCHAs in order to prevent automated use of these services.

Solve CAPTCHAs with the help of this portal, increase your business

**Follow these steps:**

Register

Login and follow the link inside to load funds to your account.

Your request will be processed ASAP.

**You pay for correctly recognized CAPTCHAs only**

The price is \$2 for 1000 CAPTCHAs. We accept payments from \$10.

**If you use a third-party software the price could be different, contact the software vendor for more information.**

Research question: how can we discover who's solving these so cheaply?

**Hi! I want to bypass captcha from my bots. Bots have different IPs. Is it possible to use your service from many IPs?**

We have no restrictions about IP: with DeCaptcher you can bypass CAPTCHA from as many IPs as you need.

**Hi. I need to crack captcha. Do you provide a captcha decoders?**

DeCaptcher CAPTCHA solving is processed by humans. So the accuracy is much better than an automated captcha solver ones

Language	Example	AG	BC	BY	CB	DC	IT	All
----------	---------	----	----	----	----	----	----	-----

Researchers *purchased* CAPTCHA solving from a range of services



Language	Example	AG	BC	BY	CB	DC	IT	All
----------	---------	----	----	----	----	----	----	-----

Solving accuracy varied by program  
and web service (e.g., Paypal or Gmail)  
... but generally nearly 90%

Language	Example	AG	BC	BY	CB	DC	IT	All
English	one two three	51.1	37.6	4.76	40.6	39.0	62.0	39.2
Chinese (Simp.)	一 二 三	48.4	31.0	0.00	68.9	26.9	35.8	35.2
Chinese (Trad.)	一 二 三	52.9	24.4	0.00	63.8	30.2	33.0	34.1
Spanish	uno dos tres	1.81	13.8	0.00	2.90	7.78	56.8	13.9
Italian	uno due tre	3.65	8.45	0.00	4.65	5.44	57.1	13.2
Tagalog	isá dalawá tatlo	0.00	5.79	0.00	0.00	7.84	57.2	11.8
Portuguese	um dois três	3.15	10.1	0.00	1.48	3.98	48.9	11.3
Russian	один два три	24.1	0.00	0.00	11.4	0.55	16.5	8.76
Tamil	ஒன்று இரண்டு மூன்று	2.26	21.1	3.26	0.74	12.1	5.36	7.47
Dutch	een twee drie	4.00	1.36	0.00	0.00	1.22	21.1	6.30
Hindi	एक दो तीन	0.00	0.00	0.00	0.00	0.00	20.2	3.37
German	eins zwei drei	0.45	0.00	0.00	0.00	0.00	15.5	2.65
Malay	satu dua tiga	0.00	0.00	0.00	0.00	0.00	15.3	2.56
Vietnamese	một hai ba	0.00	0.00	0.00	0.00	0.00	15.3	2.56
Korean	일 이 삼	0.00	0.00	0.00	0.00	0.00	20.2	3.37
Greek	ένα δύο τρία	0.45	0.00	0.00	0.00	0.00	15.5	2.65
Arabic	واحد اثنان ثلاثة	0.00	0.00	0.00	0.00	0.00	15.3	2.56
Bengali	এক দুই তিন	0.45	0.00	9.89	0.00	0.00	0.00	1.72
Kannada	ಒಂದು ಎರಡು ಮೂರು	0.91	0.00	0.00	0.00	0.55	6.14	1.26
Klingon	ᑭᑭᑭ	0.00	0.00	0.00	0.00	0.00	1.12	0.19
Farsi	یک دو سه	0.45	0.00	0.00	0.00	0.00	0.00	0.08

Also created custom CAPTCHAs requiring providing transcription of digits spelled in different languages

Table 2: Percentage of responses from the services with correct answers for the language CAPTCHAs.

Language	Example			AG	BC	BY	CB	DC	IT	All
English	one	two	three	51.1	37.6	4.76	40.6	39.0	62.0	39.2
Chinese (Simp.)	一	二	三	48.4	31.0	0.00	68.9	26.9	35.8	35.2
Chinese (Trad.)	一	二	三	52.9	24.4	0.00	63.8	30.2	33.0	34.1
Spanish	uno	dos	tres	1.81	13.8	0.00	2.90	7.78	56.8	13.9
Italian	uno	due	tre	3.65	8.45	0.00	4.65	5.44	57.1	13.2
Tagalog	isá	dalawá	tatló	0.00	5.79	0.00	0.00	7.84	57.2	11.8
Portuguese	um	dois	três	3.15	10.1	0.00	1.48	3.98	48.9	11.3
Russian	один	два	три	24.1	0.00	0.00	11.4	0.55	16.5	8.76
Tamil	ஒன்று	இரண்டு	மூன்று	2.26	21.1	3.26	0.74	12.1	5.36	7.47
Dutch	een	twee	drie	4.00	1.26	0.00	0.00	1.22	31.1	6.30
Hindi	एक	दो	तीन	0.00	0.00	0.00	1.52	6.30	9.49	5.94
German	ein	zwei	drei	0.00	0.00	0.00	1.46	0.58	29.1	5.91
Malay	satu	dua	tiga	0.00	1.42	0.00	0.00	0.55	29.4	5.23
Vietnamese	một	hai	ba	0.46	2.07	0.00	0.00	1.74	18.1	3.72
Korean	일	이	삼	0.00	0.00	0.00	0.00	0.00	20.2	3.37
Greek	ένα	δύο	τρία	0.45	0.00	0.00	0.00	0.00	15.5	2.65
Arabic	واحد	اثنين	ثلاثة	0.00	0.00	0.00	0.00	0.00	15.3	2.56
Bengali	এক	দুই	তিন	0.45	0.00	9.89	0.00	0.00	0.00	1.72
Kannada	ಒಂದು	ಎರಡು	ಮೂರು	0.91	0.00	0.00	0.00	0.55	6.14	1.26
Klingon	ᑭᑭ	ᑭᑭ	ᑭᑭ	0.00	0.00	0.00	0.00	0.00	1.12	0.19
Farsi	یک	دو	سه	0.45	0.00	0.00	0.00	0.00	0.00	0.08

Enables inference of  
*workforce demographics*

Table 2: Percentage of responses from the services with correct answers for the language CAPTCHAs.

Language	Example			AG	BC	BY	CB	DC	IT	All
English	one	two	three	51.1	37.6	4.76	40.6	39.0	62.0	39.2
Chinese (Simp.)	一	二	三	48.4	31.0	0.00	68.9	26.9	35.8	35.2
Chinese (Trad.)	一	二	三	52.9	24.4	0.00	63.8	30.2	33.0	34.1
Spanish	uno	dos	tres	1.81	13.8	0.00	2.90	7.78	56.8	13.9
Italian	uno	due	tre	3.65	8.45	0.00	4.65	5.44	57.1	13.2
Tagalog	isá	dalawá	tatló	0.00	5.79	0.00	0.00	7.84	57.2	11.8
Portuguese	um	dois	três	3.15	10.1	0.00	1.48	3.98	48.9	11.3
Russian	один	два	три	24.1	0.00	0.00	11.4	0.55	16.5	8.76
Tamil	ஒன்று	இரண்டு	மூன்று	2.26	21.1	3.26	0.74	12.1	5.36	7.47
Dutch	een	twee	drie	4.09	1.36	0.00	0.00	1.22	31.1	6.30
Hindi	एक	दो	तीन	10.5	5.38	2.47	1.52	6.30	9.49	5.94
German	eins	zwei	drei	3.62	0.72	0.00	1.46	0.58	29.1	5.91
Malay	satu	dua	tiga						9.4	5.23
Vietnamese	một	hai	ba						8.1	3.72
Korean	일	이	삼						0.2	3.37
Greek	ένα	δύο	τρία						5.5	2.65
Arabic	واحد	اثنين	ثلاثة						5.3	2.56
Bengali	এক	দুই	তিন	0.45	0.00	9.89	0.00	0.00	0.00	1.72
Kannada	ಒಂದು	ಎರಡು	ಮೂರು	0.91	0.00	0.00	0.00	0.55	6.14	1.26
Klingon	ᑭ	ᑭᑭ	ᑭᑭᑭ	0.00	0.00	0.00	0.00	0.00	1.12	0.19
Farsi	یک	دو	سه	0.45	0.00	0.00	0.00	0.00	0.00	0.08

The best (and most \$\$)  
service's workers even  
managed to learn some  
Klingon!

Table 2: Percentage of responses from the services with correct answers for the language CAPTCHAs.



Language	Example	AG	BC	BY	CB	DC	IT	All
English	one two three	51.1	37.6	4.76	40.6	39.0	62.0	39.2
Chinese (Simp.)	一 二 三	48.4	31.0	0.00	68.9	26.9	35.8	35.2
Chinese (Trad.)	一 二 三	52.9	24.4	0.00	63.8	30.2	33.0	34.1
Spanish	uno dos tres	1.81	13.8	0.00	2.90	7.78	56.8	13.9
Italian	uno due tre	3.65	8.45	0.00	4.65	5.44	57.1	13.2
Tagalog	isá					7.84	57.2	11.8
Portuguese	um					3.98	48.9	11.3
Russian	один					0.55	16.5	8.76
Tamil	ஒன்று					12.1	5.36	7.47
Dutch	een					1.22	31.1	6.30
Hindi	एक					6.30	9.49	5.94
German	eins zwei drei	3.62	0.72	0.00	1.46	0.58	29.1	5.91
Malay	satu dua tiga	0.00	1.42	0.00	0.00	0.55	29.4	5.23
Vietnamese	một hai ba	0.46	2.07	0.00	0.00	1.74	18.1	3.72
Korean	일 이 삼	0.00	0.00	0.00	0.00	0.00	20.2	3.37
Greek	ένα δύο τρία	0.45	0.00	0.00	0.00	0.00	15.5	2.65
Arabic	واحد اثنان ثلاثة	0.00	0.00	0.00	0.00	0.00	15.3	2.56
Bengali	এক দুই তিন	0.45	0.00	9.89	0.00	0.00	0.00	1.72
Kannada	ಒಂದು ಎರಡು ಮೂರು	0.91	0.00	0.00	0.00	0.55	6.14	1.26
Klingon	ᑭᑭᑭ	0.00	0.00	0.00	0.00	0.00	1.12	0.19
Farsi	یک دو سه	0.45	0.00	0.00	0.00	0.00	0.00	0.08

**Outsourcing makes  
bot-or-not problem  
fundamentally hard**

Table 2: Percentage of responses from the services with correct answers for the language CAPTCHAs.

# Project Status Reports

- Due: Fri. Apr 10 (evening)
- Goal is diagnostic (not graded)
- Along with initial sketch/reminder of project:
  - What work completed
  - What remains
  - Open issues
  - Need for a potential meeting
- Presentation (Zoom) slot preferences:
  - Tue Apr 21, Fri Apr 24, Tue Apr 28, Fri May 1

# Botnets

# Botnets: Subversion-at-Scale

- Similar to worms:
  - Spreading  $\perp$  C&C  $\perp$  Employment (if C&C flexible)
- Grew out of IRC wars/vandals (late 90s/00s)
- Broadcast-based message protocol provided easy path for control protocols



Client: PASS \$!0@  
Client: NICK [NIP]-IBM6N4SKA  
Client: USER YSNARFAL "ask0.org" "FCK" :YSNARFAL  
Client: JOIN #mipsel %#8b

Server: :[NIP]-IBM6N4SKA!YSNARFAL@114-30-XXX-XX.ip.adam.com.au JOIN  
:#mipsel

Server: :leaf.4714.com 332 [NIP]-IBM6N4SKA #mipsel :.silent on .killall  
.lscan .rlscan .esel [US],[FR],[IT],[GB],[ES],[DE] rejoin 10800 10800

Server: :leaf.4714.com 333 [NIP]-IBM6N4SKA #mipsel DRS 1228994845

Server: :leaf.4714.com 334 [NIP]-IBM6N4SKA @ #mipsel :[NIP]-IBM6N4SKA

Server: :leaf.4714.com 366 [NIP]-IBM6N4SKA #mipsel :End of /NAMES list.

Channel for bots  
running on MIPS  
architecture

```
Client: PASS $!0@
Client: NICK [NIP]-IBM6N4SKA
Client: USER YSNARFAL "ask0.org" "FCK" :YSNARFAL
Client: JOIN #mipsel %#8b
```

```
Server: :[NIP]-IBM6N4SKA!YSNARFAL@114-30-XXX-XX.ip.adam.com.au JOIN
:#mipsel
```

```
Server: :leaf.4714.com 332 [NIP]-IBM6N4SKA #mipsel :.silent on .killall
.lscan .rlscan .esel [US],[FR],[IT],[GB],[ES],[DE] rejoin 10800 10800
```

```
Server: :leaf.4714.com 333 [NIP]-IBM6N4SKA #mipsel
```

```
Server: :leaf.4714.com 353 [NIP]-IBM6N4SKA @
```

```
Server: :leaf.4714.com 366 [NIP]-IBM6N4SKA #mipsel
```

Stop what you're  
doing and reset for  
new commands

Client: PASS \$!0@  
Client: NICK [NIP]-IBM6N4SKA  
Client: USER YSNARFAL "ask0.org" "FCK" :YSNARFAL  
Client: JOIN #mipsel %#8b

Server: :[NIP]-IBM6N4SKA!YSNARFAL@114-30-XXX-XX.ip.adam.com.au JOIN  
:#mipsel

Server: :leaf.4714.com 332 [NIP]-IBM6N4SKA #mipsel :.silent on .killall  
.lscan .rlscan .esel [US],[FR],[IT],[GB],[ES],[DE] rejoin 10800 10800

Server: :leaf.4714.com 333 [NIP]-IBM6N4SKA #mipsel DRS 1228994845

Server: :leaf.4714.com 3 [NIP]-IBM6N4SKA

Server: :leaf.4714.com 366 [NIP]-IBM6N4SKA #mipsel :End of /NAMES list.

These commands are  
only for US/European bots

```
Client: PASS $!0@
Client: NICK [NIP]-IBM6N4SKA
Client: USER YSNARFAL "ask0.org" "FCK" :YSNARFAL
Client: JOIN #mipsel %#8b
```

```
Server: :[NIP]-IBM6N4SKA!YSNARFAL@114-30-XXX-XX.ip.adam.com.au JOIN
:#mipsel
```

```
Server: :leaf.4714.com 332 [NIP]-IBM6N4SKA #mipsel :.silent on .killall
.lscan .rlscan .esel [US],[FR],[IT],[GB],[ES],[DE] rejoin 10800 10800
```

```
Server: :leaf.4714.com 333 [NIP]-IBM6N4SKA #mipsel DRS 1228994845
```

```
Server: :leaf.4714.com 353 [NIP]-IBM6N4SKA @ #
```

```
Server: :leaf.4714.com 366 [NIP]-IBM6N4SKA #mipsel .End of /NAMES list.
```

Polling parameters  
for individual bots

```
Client: PASS $!0@
Client: NICK [NIP]-IBM6N4SKA
Client: USER YSNARFAL "ask0.org" "FCK" :YSNARFAL
Client: JOIN #mipsel %#8b
```

```
Server: :[NIP]-IBM6N4SKA!YSNARFAL@114-30-XXX-XX.ip.adam.com.au JOIN
:#mipsel
```

```
Server: :leaf.4714.com 332 [NIP]-IBM6N4SKA #mipsel :.silent on .killall
.lscan .rlscan .esel [US],[FR],[IT],[GB],[ES],[DE] rejoin 10800 10800
```

```
Server: :leaf.4714.com 333 [NIP]-IBM6N4SKA #mipsel DRS 1228994845
```

```
Server: :leaf.4714.com 353 [NIP]-IBM6N4SKA @ #mipsel :[NIP]-IBM6N4SKA
```

```
Server: :leaf.4714.com 366 [NIP]-IBM6N4SKA #mipsel :End of /NAMES list.
```

.visit	- flood URL with GET requests
.scan	- scans a random range for vulnerable systems (servers)
.rscan	- scans a CIDR range for vulnerable systems
.lscan	- scans the local subnet
.lrscan	- scans a range in the local subnet
.split	- splits the workload of a scan among several bots
.sql	- scans for vulnerable MySQL servers and attempts to make them download and run URL
.pma	- scans for vulnerable phpMyAdmin and attempts to make them download and run URL
.sleep	- makes the bot sleep for the given time
.sel	- ???
.esel	- skip next part if locale is not X
.vsel	- skip next part if version is not X
.gsel	- ???
.rejoin [delay]	- cycle the channel after delay
.upgrade	- download new bot from the distribution site

These are only about 1/3  
of the possible commands

# These Particular Fearsome IRC Bots?



*It appears that Netcomm NB5 ADSL modems are not the only devices affected by this bot.*

*Modems with similar hardware configurations (unknown brands) from Italy, Brazil, Ecuador, Russia, Ukraine, Turkey, Peru, Malaysia, Columbia, India and Egypt (and likely more countries) also seem to be affected, and are spreading the bot.*

## Introduction:

The NB5 was a popular ADSL/ADSL2+ modem-router, produced by Netcomm circa 2005. The NB5 is based on the Texas Instruments TNETD7300, featuring a 32bit RISC MIPS 4KEc V4.8 processor, 2MB of flash ROM, 8MB of RAM, Ethernet + USB connectivity, and runs an embedded Linux distribution.



```
Client: PASS $!0@
Client: NICK [NIP]-IBM6N4SKA
Client: USER YSNARFAL "ask0.org" "FCK" :YSNARFAL
Client: JOIN #mipsel %#8b
```

```
Server: :[NIP]-IBM6N4SKA!YSNARFAL@114-30-XXX-XX.ip.adam.com.au JOIN
:#mipsel
```

```
Server: :leaf.4714.com 332 [NIP]-IBM6N4SKA #mipsel :.silent on .killall
.lscan .rlscan .esel [US],[FR],[IT],[GB],[ES],[DE] rejoin 10800 10800
```

```
Server: :leaf.4714.com 333 [NIP]-IBM6N4SKA #mipsel DRS 1228994845
```

```
Server: :leaf.4714.com 353 [NIP]-IBM6N4SKA @ #mipsel :[NIP]-IBM6N4SKA
```

```
Server: :leaf.4714.com 366 [NIP]-IBM6N4SKA #mipsel :End of /NAMES list.
```

```
.visit          - flood URL with GET requests
.scan           - scans a random range for vulnerable routers/modems
.rscan          - scans a CIDR range for vulnerable routers/modems
.lscan          - scans the local subnet for vulnerable routers/modems
.lrscan         - scans a range in the local subnet for vulnerable routers/modems
.split          - splits the workload of a scan thread into two threads
.sql            - scans for vuln... to make them download and run URL
.pma            - scans for vuln... to make them download and run URL
.sleep          - makes th...
.sel            - ???
.esel           - skip next part if locale is not X
.vsel           - skip next part if version is not X
.gsel           - ???
.rejoin [delay] - cycle the channel after delay
.upgrade        - download new bot from the distribution site
```

Controlled spreading

```
Client: PASS $!0@
Client: NICK [NIP]-IBM6N4SKA
Client: USER YSNARFAL "ask0.org" "FCK" :YSNARFAL
Client: JOIN #mipsel %#8b
```

```
Server: :[NIP]-IBM6N4SKA!YSNARFAL@114-30-XXX-XX.ip.adam.com.au JOIN
:#mipsel
```

```
Server: :leaf.4714.com 332 [NIP]-IBM6N4SKA #mipsel :.silent on .killall
.lscan .rlscan .esel [US],[FR],[IT],[GB],[ES],[DE] rejoin 10800 10800
```

```
Server: :leaf.4714.com 333 [NIP]-IBM6N4SKA #mipsel DRS 1228994845
```

```
Server: :leaf.4714.com 353 [NIP]-IBM6N4SKA @ #mipsel :[NIP]-IBM6N4SKA
```

```
Server: :leaf.4714.com 366 [NIP]-IBM6N4SKA #mipsel :End of /NAMES list.
```

Also looks for vulnerable servers, sniffs traffic for username/passwords

```
.visit          - flood URL
.scan           - scans a C
.rscan          - scans a C
.lscan          - scans a C
.lrscan         - scans a C
.split          - splits the workload of a scan thread into two threads
.sql            - scans for vulnerable MySQL servers and attempts to make them download and run URL
.pma            - scans for vulnerable phpMyAdmin and attempts to make them download and run URL
.sleep          - makes the bot sleep for the given time
.sel            - ???
.esel           - skip next part if locale is not X
.vsel           - skip next part if version is not X
.gsel           - ???
.rejoin [delay] - cycle the channel after delay
.upgrade        - download new bot from the distribution site
```



More Sophisticated C&C

# Welcome to Storm!

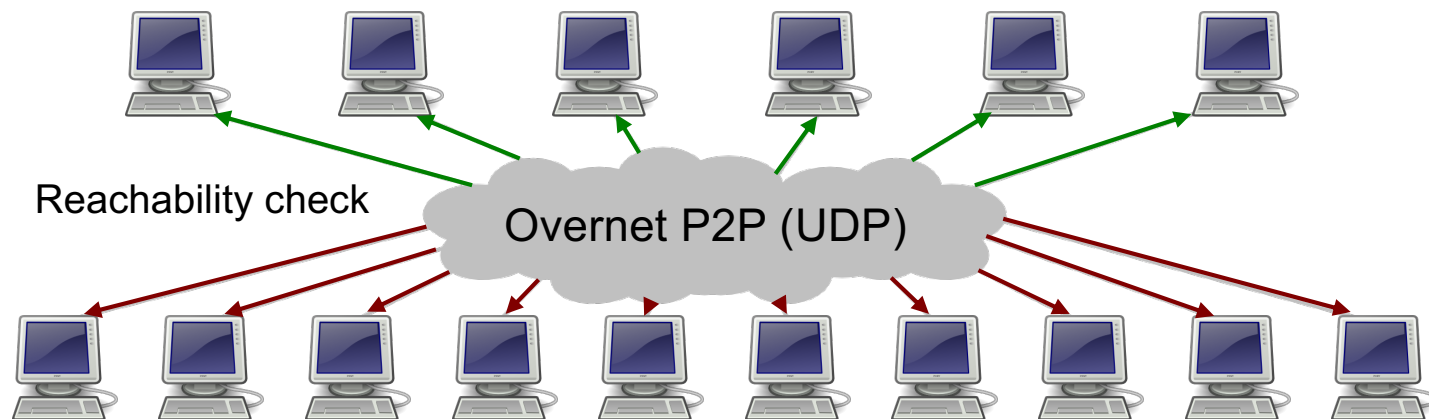


# The Storm botnet

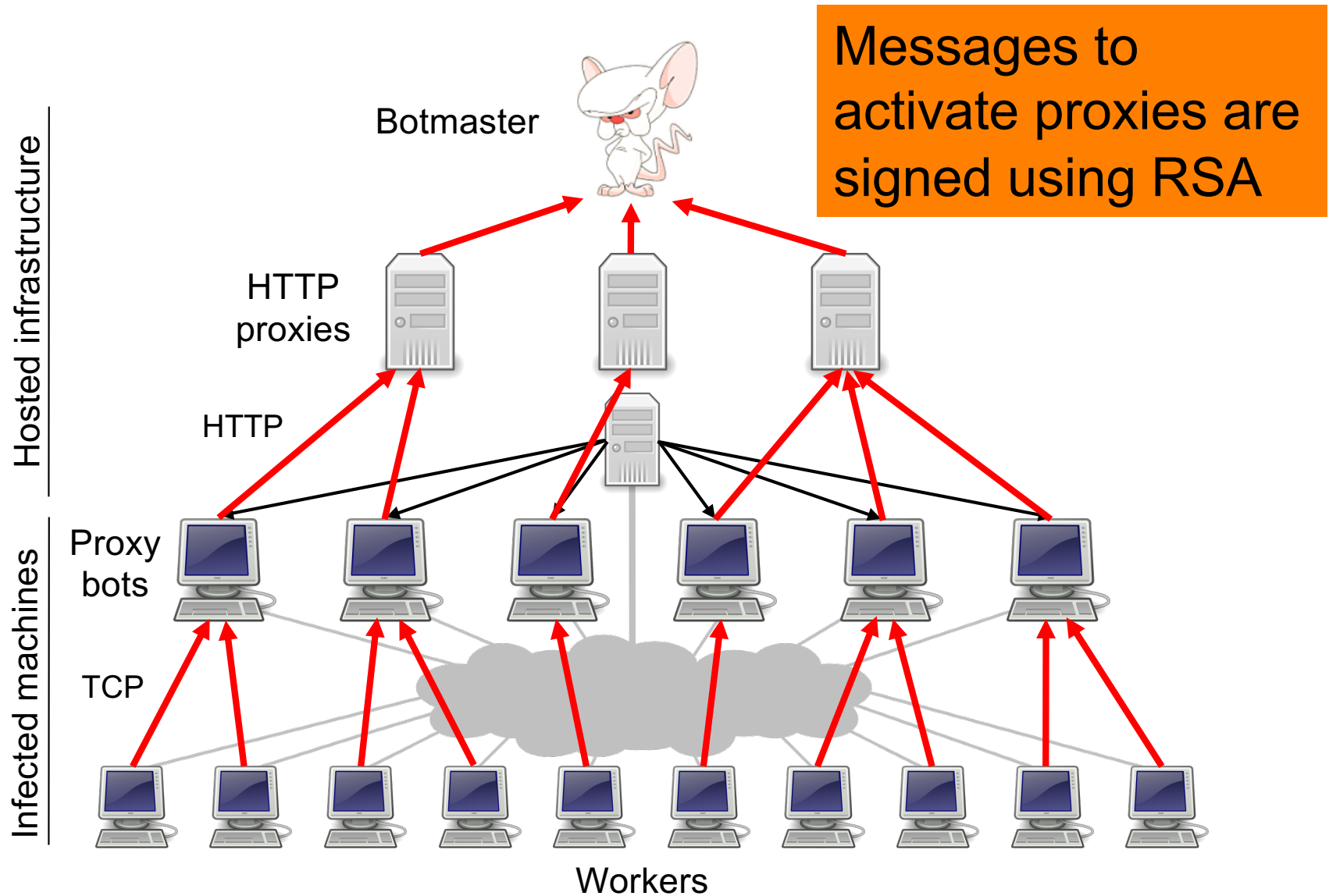
Each bot generates its own  
128-bit Overnet ID (OID)

Finds Overnet peer  
with closest OID

Existing Overnet node checks  
new bot for reachability (= no NAT)



# The Storm botnet



September 6th, 2007

# Storm Worm botnet could be world's most powerful supercomputer

Posted by Ryan Naraine @ 8:41 am

**Categories:** [Botnets](#), [Browsers](#), [Data theft](#), [Exploit code](#), [Firefox.....](#)

**Tags:** [Operation](#), [Supercomputer](#), [Malware](#), [Worm](#), [Ryan Naraine](#)



**150** TalkBacks

ADD YOUR OPINION



SHARE



PRINT



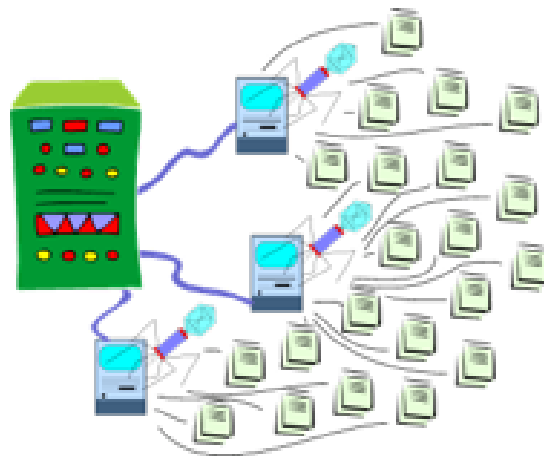
E-MAIL



**+97**

WORTHWHILE?

115 VOTES



Nearly nine months after it was first discovered, the [Storm Worm](#) Trojan continues to surge, building what experts believe could be the world's most powerful supercomputer.

The Trojan, which uses a myriad of social engineering lures to trick Windows users into downloading malware, has successfully seeded a massive botnet — between one million and 10 million CPUs — producing computing power

to rival the world's top 10 supercomputers

“

*The [Storm] botnet reportedly is powerful enough as of September 2007 to force entire countries off the Internet, and is estimated to be capable of executing more instructions per second than some of the world's top supercomputers. However, it is not a completely accurate comparison, according to security analyst James Turner, who said that comparing a botnet to a supercomputer is like comparing an army of snipers to a nuclear weapon*

“

*At certain points in time, the Storm worm used to spread the botnet has attempted to release hundreds or thousands of versions of itself onto the Internet, in a concentrated attempt to overwhelm the defenses of anti-virus and malware security firms. According to Joshua Corman, an IBM security researcher, "This is the first time that I can remember ever seeing researchers who were actually afraid of investigating an exploit."*

# How Big Was *Storm*?

Bots make 16 calls to this,  
taking bottom 8 bits each time,  
to construct 128-bit OID

(PRNG). Storm generates OIDs using its own PRNG  
given by the recurrence:

Issues?

$$I_{i+1} = (a \cdot I_i + b \bmod 2^{32}) \bmod m$$

with  $a = 1664525$ ,  $b = 1013904223$ ,  $m = 32767$ , and  
the initial value  $I_0$  is based on the system clock. The  
generator appears to be based on a well-known linear  
congruential PRNG described in the *Numerical Recipes*

Only 32,767 possible OIDs!

# Do All OIDs Come From Limited Pool?

Location	Hallmarks
Germany	Random OIDs with lower 10 bytes constant. Floods the Storm network aggressively with thousands of fake node IPs.
Iran	Random OIDs biased to upper half of space (first bit always set).
Sweden	Random OIDs biased to upper half of space (first bit always set). Does not appear in routing tables of any other peers.
France	One fixed OID, relatively passive crawler, appears to just be sampling Storm.
East Coast, US	257 OIDs evenly distributed in ID space behind one IP, port number used as upper two bytes of the OID.
East Coast, US	Uniform random OIDs, both a Storm implementation and crawler behind the same IP, does not report other peers.
West Coast, US	Random OIDs biased to upper half of space 100:1. Does not report IPs in response to queries.

Table 2: Other parties participating in the “encrypted” Storm network on April 4, 2008.

Lots of *poisoning/probing*



# How Big Was *Storm*?

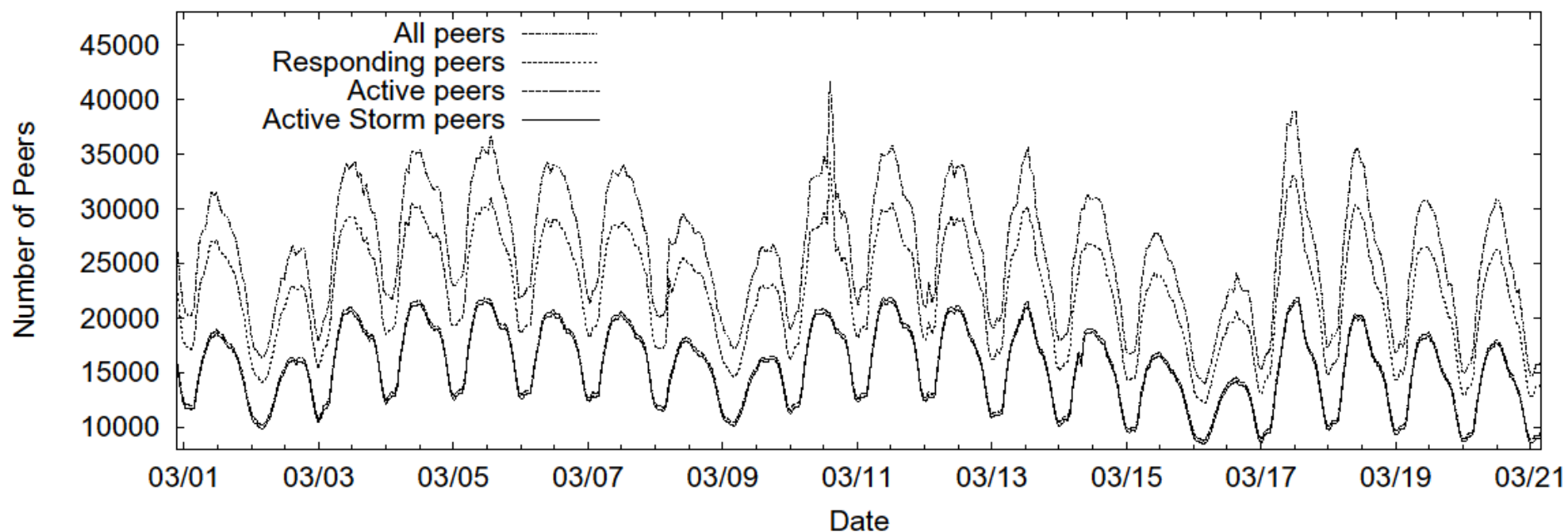
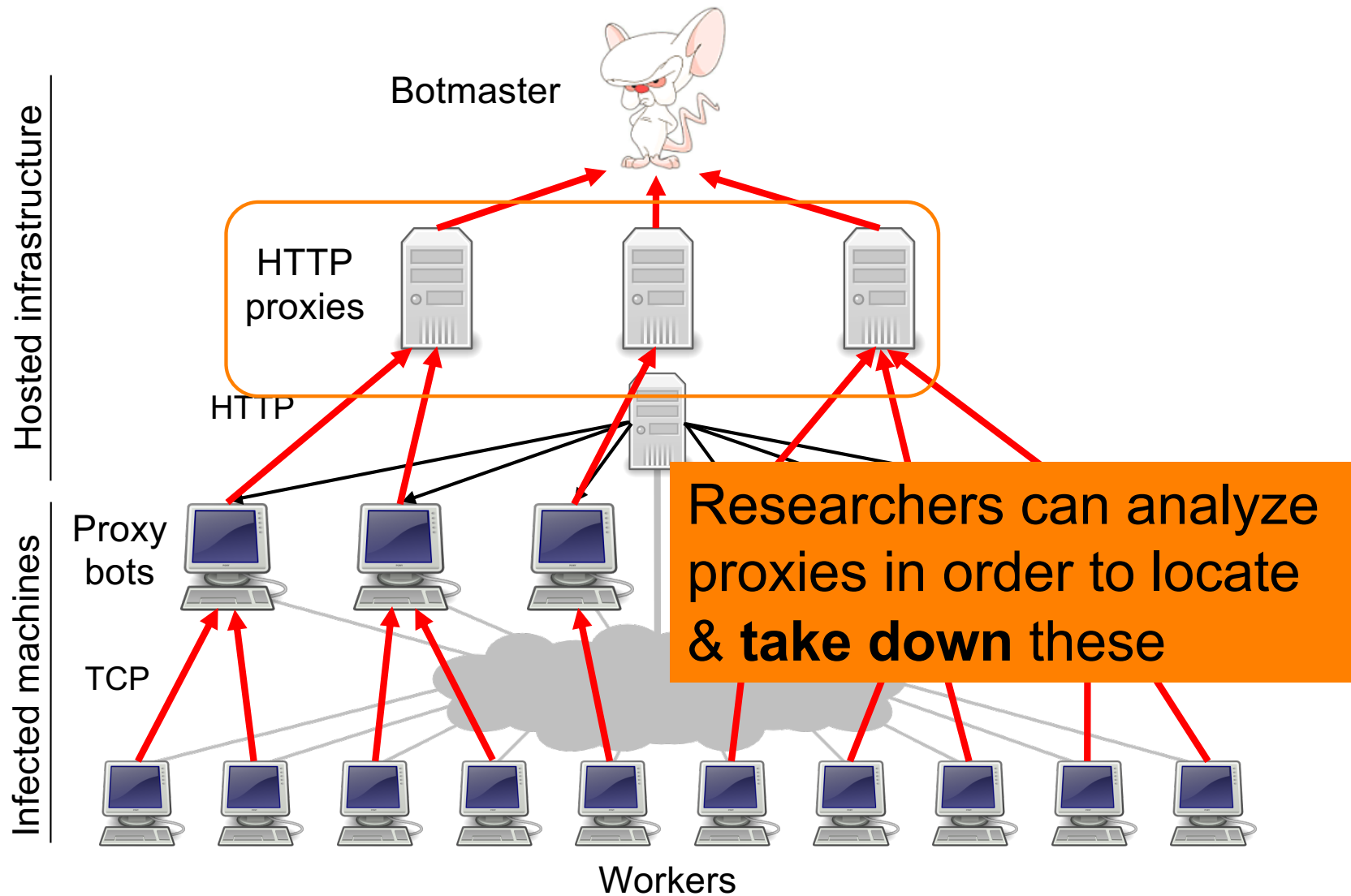


Figure 2: Estimates of the size of the Storm botnet using different notions of liveness over the first three weeks of March 2008  
Note that the  $y$ -axis does not begin at zero to better separate the curves.

# The Storm botnet

Vulnerabilities?



# Other Ways to Find C&C Infrastructure?

## MegaD C&C's crafted response to "GET /"

```
HTTP/1.0 200 OK Server: Apache/1.3.37  
Content-Type: text/html; charset=iso-8859-1
```

```
<html>  
  <head>  
    <title> test page </title>  
  </head>  
  <body>  
    <a href='http://www.microsoft.com/'>microsoft.com</a>  
  </body>  
</html>
```

Huh what happens if we google on pages that look just like this?

Web

[+ Show options...](#)

Results 1 - 6 of 6 for l

[test page](#)

microsoft.com.

doretorza.com/ - [Cached](#)

[test page](#)

microsoft.com.

www.doretorza.com/ - [Cached](#)

[test page](#)

microsoft.com.

selementusaks.org/ - [Ca](#)

[test page](#)

microsoft.com.

kildamindak.net/ - [Cached](#)

[test page](#)

microsoft.com.

www.kildamindak.net/ - [Cached](#)

[test page](#)

microsoft.com.

216.32.90.186/

Botmaster countermeasures to  
avoid C&C server takedown?  
(in addition to DGAs)



**GooHost.ru**  
Reliable and quality hosting

Тел.: +7(495) 542-39-87, icq: 418396204

#### Menu

- Hosting Plans
- Email Mailing
- Website Design
- FAQ
- Dedicated server
- Domain Registration
- Payment
- Contact

## Hosting Plans

We offer a complaint-resistant hosting to host your sites, which are specified in mass mailings.

We decided to bring visitors to your web site through unsolicited mass emails? Wonderful idea! You certainly expect a boom visits. But! As in any ointment and then not pass without a spoon of tar ... Alas, but your wonderful site, shortly after the start of spam mail, will be closed due to flood of complaints from postal services. Is there a way to avoid these problems? Of course! Our complaint-resistant hosting simply ignores any complaints, all postal services, and you can be rest assured about the performance of their sites - they will not be closed. And you get new customers, expand their business and increase their sales and revenue, thanks to spam mailing lists.



Наш хостинг  
работает  
24 в сутки!

**Obuzoustoychivy hosting** is more expensive than usual, but you will have the full guarantee that your site no one ever closes, it will always be available to your customers!

**\$125-225/month**

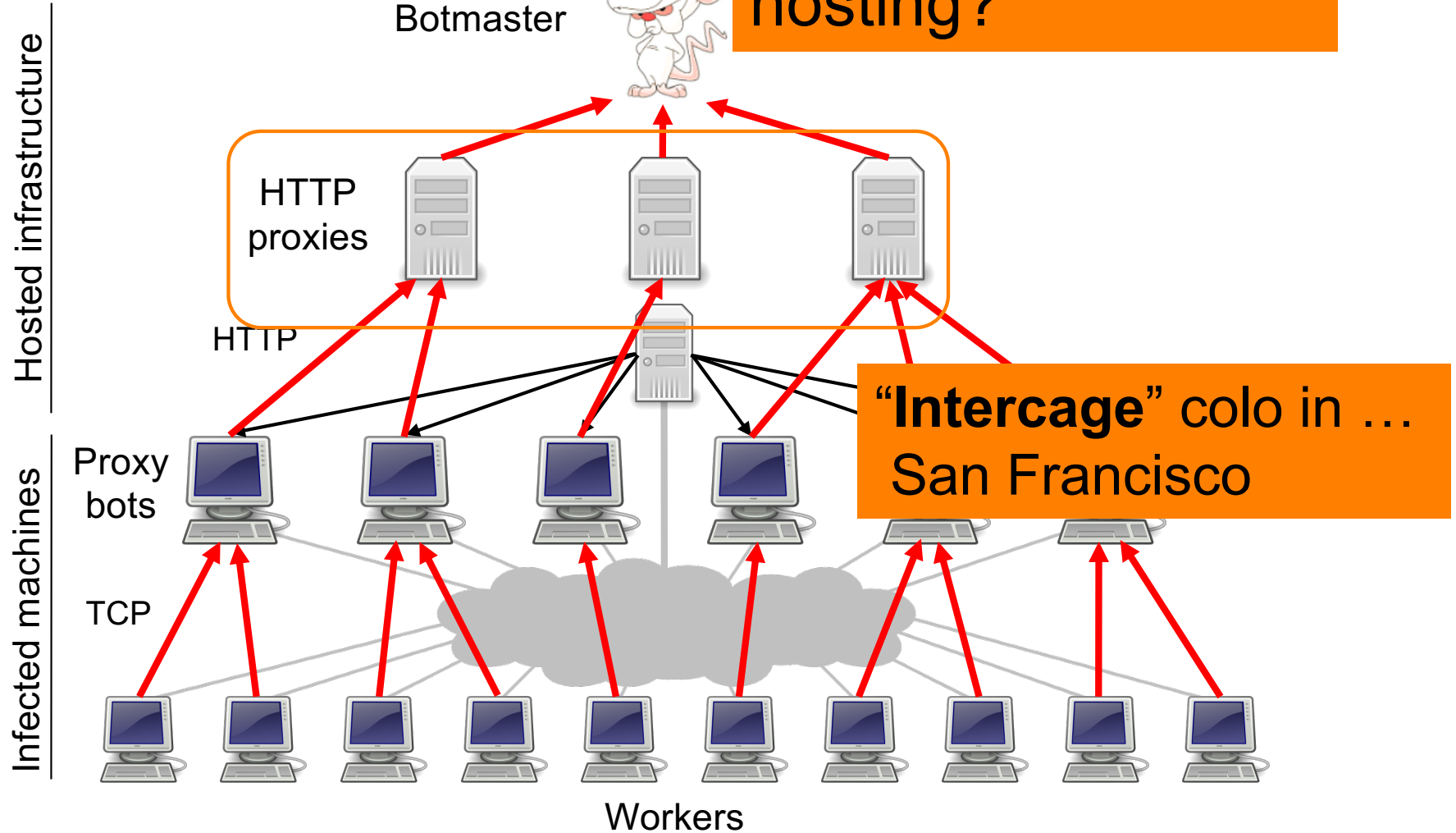
<u>MINI PLAN</u>	
Volume disc	400 MB
Domains	1
Traffic *	Unlimited
FTP-access	there is
MySQL database	there is
Control panel	there is
COST	4 000 rub. / 1 month.

<u>STARTER PLAN</u>	
Volume disc	500 mb
Domains	3
Traffic *	Unlimited
FTP-access	there is
MySQL database	there is
Control panel	there is
COST	5 000 rub. / 1 month.

<u>BUSINESS PLAN</u>	
Volume disc	1000 mb
Domains	7
Traffic *	Unlimited
FTP-access	there is
MySQL database	there is
Control panel	there is
COST	7 000 rub. / 1 month.

<u>PREMIUM PLAN</u>	
---------------------	--

# The Storm botnet







## Security Fix

Brian Krebs on Computer Security

[About This Blog](#) | [Archives](#) | [Security Fix Live: Web Chats](#) | [E-Mail Brian Krebs](#)

### SEARCH THIS BLOG

Go

### RECENT POSTS

- [E-Banking on a Locked Down PC, Part II](#)
- [ChoicePoint Breach Exposed 13,750 Consumer Records](#)
- [President Obama on Cyber Security Awareness](#)
- [Mozilla Disables Microsoft's Insecure Firefox Add-on](#)
- [PayChoice Suffers Another Data Breach](#)

### Entries By Category

- [Cyber Justice](#)
- [Economy Watch](#)
- [Fraud](#)
- [From the Bunker](#)
- [Latest Warnings](#)
- [Misc.](#)
- [New Patches](#)
- [Piracy](#)
- [Safety Tips](#)

## Spam Volumes Drop by Two-Thirds After Firm Goes Offline

The volume of junk e-mail sent worldwide plummeted on Tuesday after a Web hosting firm identified by the computer security community as a major host of organizations engaged in spam activity was taken offline. (Note: A link to the full story on McColo's demise is available [here](#).)



Experts say the precipitous drop-off in spam comes from Internet providers unplugging **McColo Corp.**, a hosting provider in Northern California that was the home base for machines responsible for coordinating the sending of roughly 75 percent of all spam each day.

In an alert sent out Wednesday morning, e-mail security firm **IronPort** said:

In the afternoon of Tuesday 11/11, IronPort saw a drop of almost 2/3 of overall spam volume, correlating with a drop in IronPort's SenderBase queries. While we investigated what we thought might be a technical problem, a major spam network, McColo Corp., was shutdown, as reported by The Washington Post on Tuesday evening.

Spamcop.net's graphic [shows a similar decline](#), from about 40 spam e-





# Security Fix

Brian Krebs on Computer Security

[About This Blog](#) | [Archives](#) | [Security Fix Live: Web Chats](#) | [E-Mail Brian Krebs](#)

## SEARCH THIS BLOG

Go

## RECENT POSTS

- [Farewell 2009, and The Washington Post](#)
- [Hackers exploit Adobe Reader flaw via comic strip syndicate](#)
- [Twitter.com hijacked by 'Iranian cyber army'](#)
- [Group IDs hotbeds of Conficker worm outbreaks](#)
- [Hackers target unpatched Adobe Reader, Acrobat flaw](#)

## Entries By Category

- [Cyber Justice](#)
- [Economy Watch](#)
- [Fraud](#)
- [From the Bunker](#)
- [Latest Warnings](#)

## Retail Fraud Rates Plummeted the Night McColo Went Offline

One month after the [shutdown of hosting provider McColo Corp.](#), spam volumes are nearly back to the levels seen prior to the company's take down by its upstream Internet providers. But according to one noted fraud expert, spam wasn't the only thing that may have been routed through the Silicon Valley based host: New evidence found that retail fraud dropped significantly on the same day.

It is unclear whether the decrease in retail fraud is related to the McColo situation, but in speaking with **Ori Eisen**, founder of [41st Parameter](#), he said close to a quarter of a million dollars worth of fraudulent charges that his customers battle every day came to a halt.

Eisen, whose company provides anti-fraud consulting to a number of big retailers and banks, told me at least two of the largest retailers his company serves reported massive declines in fraud rates directly following McColo's termination.

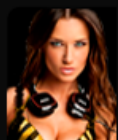
"It stopped completely that night," Eisen said, referring to a drop in fraudulent activity linked to purchases of high-value merchandise with stolen credit and debit cards on Nov. 11, the day McColo was shut down. "Yet, it will come back after [the scammers] erect their new infrastructure."

# How Bulletproof Hosting Looks in Recent Times



# bulletproof hosting BulletProof Web

"exceeding expectations"



Write us:

LIVE CHAT

CREATE TICKET



[Client Area](#)

[FAQ](#)

[Offers](#)

[Terms](#)

[Partnership](#)

[About](#)

[News](#)

[Blog](#)

[BulletProof Servers](#)

[BulletProof VPS](#)

[BulletProof Domains](#)

[DDoS Protection](#)

[VPN](#)

Promo code:

**BEPROTECTED**

**10% OFF** discount on Protection against DDoS attacks

Expires after **8 days**

**Bulletproof hosting**

[Blog](#)

[Offers](#)

[News](#)

08.04.2016

[Regular Hosting Fails](#)

[35% discount on bulletproof servers and VPS](#)

Use promo NICETOMEETYOU and get 35%...

15.04.2015

[Hello world!](#)





# bulletproof hosting BulletProof Web

"exceeding expectations"



Write us:

LIVE CHAT

CREATE TICKET



[Client Area](#)

[FAQ](#)

[Offers](#)

[Terms](#)

[Partnership](#)

[About](#)

[News](#)

[Blog](#)

BulletProof Servers

BulletProof VPS

BulletProof Domains

DDoS Protection

VPN

in CyberBunker

in Netherlands

in Moldova

in Russia

in Ukraine

in Sweden

Promo code:

**BEPROTECTED**

**10% OFF** discount on Protection against  
DDoS attacks

Expires after **8 days**

**Bulletproof hosting**

[Blog](#)

[Offers](#)

[News](#)

08.04.2016

[BulletProof-Servers/](#) [a Fails](#)

<https://bpw.sc/BulletProof-Servers/>

[35% discount on bulletproof servers and VPS](#)

Use promo NICETOMEETYOU and get 35%...

15.04.2015

[Hello world!](#)

# BulletProof Server in Ukraine



fm. \$399 USD



Getting a **bulletproof server in Ukraine** is actually a really good idea if you have limited options. If you can't use servers in Russia or in other European countries, a Ukraine bulletproof server is an excellent choice.

The best part about bulletproof servers in Ukraine is its loose rules in content. You won't have to worry about third parties complaining about your content because it's pretty much a haven for internet marketers operating any form of business online.

Add in the fact that traffic cost is relatively low, getting a bulletproof server in Ukraine makes so much sense for your business. Avail our special offer today!

[Restrictions](#)

## Configurable Options

Processor:

2x intel Xeon L5520



Memory:

24 Gb +\$50



Discs:

2000 Gb +\$45



Network:

100 Mb/s (unlim.)



Dedicated IP:

4 +\$30



Operating System:

FreeBSD-10-amd64



Panel:

ISPmanager +\$20



Backup size:

5 Gb +\$10



Administration:

Optimum +\$50



Order now!

Subtotal: \$604



# BulletProof VPS in Netherlands



fm. \$90 USD



If you want a truly authentic European quality connectivity, then our **bulletproof VPS in Netherlands** is the perfect pick for you.

With our promise of 100% uptime, you are getting an unbelievable deal. Because Netherlands have very friendly laws when it comes to content distribution, you can run websites and businesses that may contain sensitive content within Europe.

Simply put – if a certain content is banned to operate in other EU countries, it's probably legal in Netherlands. So if you want a piece of that business, going with a **Bulletproof VPS in Netherlands** is a move you should make.

You can enjoy stellar security, uptime, privacy, and smooth operations from start to finish with our **Netherlands bulletproof VPS service**. Contact us today and feel the difference!

[Restrictions](#)

## Configurable Options

Processor:	2 core Intel Xeon E3 1230 +\$40
Memory:	2048 MiB +\$10
Discs:	100 Gb +\$20
Network:	unlimited (100Mb/s)
Dedicated IP:	2 +\$15
Operating System:	CentOS-6-amd64
Panel:	ISPmanager +\$20
Backup size:	5 Gb +\$10
Administration:	Optimum +\$50

Order now!

Subtotal: \$255





# DDoS Protection



fm. \$295 USD

Do you need an additional protection for your resource?

Are rivals and ill-wishers trying to disable it?

Our service for **protection against DDoS attacks** will put your mind at ease and help you forget about such problems once and for all!

The most powerful protection will **defeat a DDoS attack** of up to 180 Gbps and 120 million Pps.

## Configurable Options

Anti-DDoS:

IP protection +\$489

☒ IP protection +\$489

Domain protection

## Billing Cycle

☒ 1 mo. ☐ 3 mo. ☐ 6 mo. ☐ yearly

Total Due Today: \$784  
Total Recurring Monthly: \$784

Checkout »



Customer Service



# Bulletproof domain registration



fm. 35 USD

**Registration of bulletproof domains** is conducted by our partners based in China. The reliability of our partners is clearly highlighted by over 5 years of our collaboration and thousands of registered domains.

**Bulletproof domains** are a must-have for undertaking projects with ample and fierce competition. With **bulletproof domains**, your project will finally be able to function, undeterred by adversaries' attempts to block it through complaints to the domain registrar, while other domains registered from ordinary registrars get blocked in the same circumstances.

Don't let yourself be pressured or threatened - **register bulletproof domains!**

Type in the domain you wish to register below to check for availability.

www.  .com



[BulletProof Domains](#)



[BulletProof Server in CyberBunker](#)

Payment  
methods



WebMoney



[FAQ](#) [Offers](#) [Terms](#) [About](#)

BulletProof Hosting since 2009 © BulletProof Web Inc.



# Bulletproof domain registration



fm. 35 USD

**Registration of bulletproof domains** is conducted by our partners based in China. The reliability of our partners is clearly highlighted by over 5 years of our collaboration and thousands of registered domains.

**Bulletproof domains** are a must-have for undertaking projects with ample and fierce competition. With **bulletproof domains**, your project will finally be able to function, undeterred by adversaries' attempts to block it through complaints to the domain registrar, while other domains registered from ordinary registrars get blocked in the same circumstances.

Don't let yourself be pressured or threatened - **register bulletproof domains!**

Type in the domain you wish to register below to check for availability.

www.

myhackersite

.com

GO!

Hello, feel free to ask me about our services, also I can provide special offer for your project, just ask me.

начать диалог

Customer Service

## Choose Domains

Domain Name	Status	More Info
myhackersite.com	<input checked="" type="checkbox"/> Available! Order Now	1 Year/s @ \$35
myhackersite.net	<input type="checkbox"/> Available! Order Now	1 Year/s @ \$35
myhackersite.org	<input type="checkbox"/> Available! Order Now	1 Year/s @ \$35
myhackersite.biz	<input type="checkbox"/> Available! Order Now	1 Year/s @ \$35
myhackersite.info	<input type="checkbox"/> Available! Order Now	1 Year/s @ \$35
myhackersite.name	<input type="checkbox"/> Available! Order Now	1 Year/s @ \$35

# About Us

## Who are we and what do we do?

Our company has been in business since 2009, when it was registered in an offshore zone of the Seychelles Islands.

Most of our work is focused on providing reliable bulletproof hosting with protection from any encroachment, maintaining our clients' rights to full freedom of information and independence.

We distribute information on trustworthy platforms in Russia, Ukraine, EU countries and China. There is plenty of room for another project on the internet – and we are prepared to provide you with it.

We have always carefully protected clients' websites from all attacks and claims. Our company policy, combined with experience, technical professionalism and time-tested arrangements with data centers guarantee that all data on our servers is fully protected from intervention by authorities, bothersome right holders, and organizations like Spamhaus.

We value and treasure freedom on the internet because this is one of the few places where it still remains.

## What are the advantages of working with us?

### Bulletproof protection

Our defining trait is our willingness to provide services which are not easily blocked by third parties. Unlike ordinary hosts, which terminate services upon receiving any sort of claim against their client, we do not let our customers be bullied. A wide variety of platforms and internal arrangements allow us to prevent attempts by ill-wishers to block your projects.

### Experience

Our team has been working in the sphere of bulletproof hosting for over five years. Throughout this period, we've dealt with the toughest problems, provided services to the most diverse clients, cooperated with the most reliable partners and now wish to attain even more experience with your help.

### An individual approach

Share your projects with us, and we will provide ideal conditions for their existence, given our skill in the technical and legal field.

We can do the following:

- Select a country whose current legislation will not impede the distribution of your materials;
- Find a platform that will best suit your requirements;
- Accept payment in any form convenient for you, including Bitcoin, which maintains the highest level of anonymity of online payments;
- Set up and configure hardware best suited for your projects;
- Provide high-quality, around-the-clock support for all of your project's stages;
- Guarantee protection from claims and abrupt failure of equipment;
- Ensure stable functioning of your project;



# Blog → Why You Need Bulletproof Hosting

Imagine yourself spending so much time, money, and resources on your internet venture. Actually, you don't even need to 'imagine' because I'm pretty sure you've spent a considerable amount of time and cash into making money online.

But if for some reason, your tactics are closer to blackhat and grayhat, then your hard work could be in jeopardy.

As you know, big companies like Google can just penalize your website whenever they please. Once they find out that you aren't exactly playing by the rules, you could get the ban hammer.

Nevermind Google... How about your own government chasing you around for running a porn tube or an online gambling site? That's a very serious issue that you surely don't want to be part of.

You could end up paying a huge amount of cash to the government, or worse — get arrested.

## Restrictions

They are few, but they do exist. We restrict ourselves within the confines of professional ethics, general human morality, and the law of countries our equipment is stationed in.

For these reasons, we do not support:

- email spam
- all forms of fraud
- child pornography
- fascism and terrorism
- violence
- activity deemed illegal in countries our equipment is stationed in



1.4 Claims regarding untimely responses with the aforementioned sources will not be considered. It is forbidden to distribute resources and conduct activity considered illegal in the countries where the servers or hosting are physically located.

1.5 When making any kind of arrangement with the company, the client is considered to be familiar with the terms of conditions of the company's services and is obligated to follow them.

## **2. Registration and maintenance of domain names**

2.1 Upon registration of domain names, the company reserves the right to present its contact information to administrators of WHOIS domain services. A written notification, as well as an ID document must be presented by the client to edit this contact information.

2.2 To refer a domain to other registrars for maintenance, a query should be submitted no later than 14 days before the termination of this domain's delegation term.

2.3 Domain registration and maintenance can be terminated due to submission of false contact information or failure to provide contact information on demand.

2.4 Domain registration and maintenance can be terminated if the client refuses the registration/domain extension service, along with cases of domain transfer and annulment of domain registration, including court-authorized action.

## **3. Termination of services**

The company reserves the right to terminate services offered to the client without monetary compensation in the following cases:

1 Violation of these rules and conditions.

2 DOS and DDOS attacks on client resources not protected by the "Anti-DDOS" system.

3 Activities (hacking, attack, etc.) aimed at unsanctioned disruption of the company servers' operation or aimed at discrediting the company. This includes court decisions and cases provided for in legislation.

## **4. Monetary compensation**

4.1 In cases where server or hosting rental is refused within a week after payment, 20% of the payment total is deducted for the installation of a server (without discounts or promotions). As an example, we can use a server with anti-DDOS protection purchased for \$450 (the standard, non-promotion price equals \$500). In the case of a refusal within a week's time, the compensation will total  $\$450 - (500 \cdot 20\%) = \$350$ .

4.2 Upon denial of domain registration or transfer, as well as any accompanying services (data protection, DNS, etc.), the payment is not compensated.

4.3 If an order is annulled due to violation of these rules, funds spent are not compensated.

4.4 If there is a lack of a technical ability to provide a paid-for service, the client's funds can be returned within 10 calendar days if he requests it.

4.5 Compensation of funds takes place within a 10 calendar day term.

## **5. Information Submission**

5.1 The client is obligated to submit accurate and truthful information in the quantity necessary for the requested services to be provided.

5.2 The client's personal information is not shared with third persons, except in cases specified in the law of countries where the servers are physically located.

## **6. The company's responsibilities before third persons**

The company bears no responsibility for the utilization of domains registered with its help, as well as the content of any materials posted under sites with these domains or

Become a partner today and start making a profit as soon as tomorrow!

### Advantages of our partnership

1. Upon registering for our partners' program, we immediately transfer a 25\$ bonus to your account.
2. High profit margins. You will receive up to 20% from each payment made by your referrals. The "average lifespan" of our clients is over half a year.
3. High commission rates. You can receive more than 200\$ from a single referral every month for some orders.
4. We have the best prices and service quality on the market, so you will easily manage to attract new referrals.

### How does the partner program work?

1. Every visitor who accesses our site via your partner's link receives cookies for a 6-month period. If he makes a purchase during this period, you will receive interest from their purchases.
2. Bonuses are transferred when making a payment for any service and they accumulate in your partner's account.
3. These bonuses can then be used to pay for our services as well as transferred to an account in the Webmoney system.
4. Минимальная сумма для использования отсутствует, для вывода — \$50.

### Scope of partners' bonuses

Number of referrals	Profit from orders
from 1 to 3	5%
from 4 to 7	10%
from 7 to 14	15%
15 >	20%

Furthermore, if you use our hosting service, you will receive a free month bonus for the first client you bring in!

### The bare facts

1. There are 70 active users currently participating in our partner program.
2. The average number of clients referred per partner is 6 people.
3. Over \$16,000 in profits have currently been made with the partner program.

[Get a \\$25 registration bonus and start earning money with Bulletproof Web!](#)

[Go to Registration](#)